AMENDMENTS OF THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1.(Currently Amended) A method for an intermediary selectively coupling an external network and an internal network to dynamically generate filter rules to facilitate establishing an end to end secure session connection between a first device on the internal network and a second device of the external network, the method comprising:

receiving a secure session establishment request by the second device on the external network to establish a secure communication session with the first device on the internal network;

forwarding the secure session establishment request to the first device;

monitoring the internal network to detect an approval or disapproval acknowledgement by the first device for the secure session establishment request; and

configuring a first filter rule of the intermediary to allow communication between the first and second devices through the intermediary, if an approval authentication acknowledgement is detected;

~~receiving~~ determining whether network traffic from the second device is corresponding to a previous secure communication session established when the second device was previously on the internal network, wherein the second device uses an address that is globally routable on the internal and the external networks and therefore said network traffic is valid with respect to the internal network; and

responding to said network traffic with an error ~~such that~~and forcing the second device ~~attempts~~ to re-establish a secure communication session from the external network.

2. (Original) The method of claim 1, further comprising:

determining a presence advertisement for the first device has been received before forwarding the secure session establishment request to the first device.

3. (Original) The method of claim 2 wherein the presence advertisement is delivered in accordance with the UPnP Simple Service Discovery Protocol (SSDP).

4. (Original) The method of claim 1, further comprising:

receiving network traffic from the second device corresponding to the second device requesting a UPnP Device Description Document from the first device.

5. (Original) The method of claim 1, further comprising:

receiving a service request from the second device for the first device, the service request having an associated communication port for performing the service;

determining the service request identifies a service advertised by the first device in a device description document; and

configuring a second filter rule to allow communication between the first device and the second device using the associated communication port.

6. (Original) The method of claim 1, further comprising:

providing the second device with an indicia for use by the second device in establishing a communication link to the first device.

7. (Cancelled)

8. (Original) The method of claim 1, wherein communication within the internal network is in accord with an IPv6 compatible Internet Protocol (IP).

9. (Original) The method of claim 1, further comprising:

retrieving an Access Control List (ACL) from the first device, the ACL including an identification of devices authorized to establish communication sessions; and

determining based at least in part on the ACL the second device is authorized to establish the secure communication session with the first device before forwarding the secure session establishment request to the first device.

10. (Cancelled)

11. (Original) The method of claim 1, further comprising:

establishing the end to end secure session connection between the first device on the internal network and the second device of the external network in a single end to end secure session connection between said first and second devices.

12.-14. (Cancelled)

15. (Cancelled)

16. -22. (Cancelled)

23. (Currently Amended) A system of devices communicatively coupled with an internal network and an external network via a gateway, comprising:

a first device, communicatively coupled to the internal network, offering services;

a second device selectively coupled with the internal and external networks and uses an address globally routable on the internal and the external network, the second device seeking a service of the first device, wherein when requesting the service, said requesting includes sending a secure communication initiation request to the first device to facilitate establishing a secure communication session with the first device; and

an intermediary selectively communicatively coupling the first and second devices, wherein the intermediary is configured to receive a secure communication initiation request from the second device over the external network and forward the request to the first device, determine whether network traffic from the second device is corresponding to a previous secure communication session established when the second device was previously on the internal network, respond to said network traffic with an error and force the second device to re-establish a secure communication session from the external network.

24. (Original) The system of claim 23, wherein the intermediary is further configured to monitor the first device for an approval or disapproval authentication acknowledgement for the request, and to configure a filter of the intermediary controlling communication over the first network from the first device based at least in part on a monitored authentication acknowledgement.

25. (Original) The system of claim 23, wherein the first device communicates with the second device in accord with the UPnP Security Protocol.

26. (Original) The system of claim 23, wherein the secure communication initiation request corresponds to a UPnP Set Session Key (SSK) request.

27. (Currently Amended) An article of manufacture comprising

a storage medium; and

a plurality of programming instructions stored on the storage medium and configured to enable a machine as an intermediary selectively coupling an external network and an internal network to dynamically generate filter rules to facilitate establishing an end tno end secure session connection between a first device on the internal network and a second device of the external network to:

receive a secure session establishment request by a second device on the external network to establish a secure communication session with a first device on the internal network;

forward the secure session establishment request to the first device;

monitor the internal network to detect an approval or disapproval acknowledgement by the first device for the secure session establishment request; and

configure a first filter rule of the intermediary to allow communication between the first and second devices through the intermediary, if an approval authentication acknowledgement is detected;

~~receive~~ determine whether network traffic from the second device is corresponding to a previous secure communication session established when the second device was previously on the internal network, wherein the second device uses an address that is globally routable on the internal and the external networks and therefore the network traffic is valid with respect to the internal network; and

respond to said network traffic with an error ~~such that~~and forcing the second device ~~attempts to~~ re-establish a secure communication session from the external network.

28. (Previously Presented) The article of manufacture of claim 27, wherein the programming instructions are further configured to enable the machine to determine a presence advertisement for the first device has been received before forwarding the secure session establishment request to the first device.

29. (Previously Presented) The article of manufacture of claim 27, wherein the programming instructions are further configured to enable the machine to receive a service request from the second device for the first device, the service request having an associated communication port for performing the service;

determine the service request identifies a service advertised by the first device in a device description document; and

configure a second filter rule to allow communication between the first device and the second device using the associated communication port.

30. (Previously Presented) The article of manufacture of claim 27, wherein the programming instructions are further configured to enable the machine to provide the second device with an indicia for use by the second device in establishing a communication link to the first device.

31. (Previously Presented) The article of manufacture of claim 27, wherein the programming instructions are further configured to enable the machine to

retrieve an Access Control List (ACL) from the first device, the ACL including an identification of devices authorized to establish communication sessions; and

determine based at least in part on the ACL the second device is authorized to establish the secure communication session with the first device before forwarding the secure session establishment request to the first device.

32. (Cancelled)

33. (Cancelled)

34.-35. (Cancelled)

36.-37. (Cancelled)